



PATENT  
Attorney Docket No.: 16869B-145900US  
Client Ref. No.: HAL269  
(340300833US01)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:

YUICHI YAGAWA

Application No.: 10/808,792

Filed: March 24, 2004

For: WORM PROVING STORAGE  
SYSTEM

Customer No.: 20350

Examiner: Mano Padmanabhan

Technology Center/Art Unit: 2188

Confirmation No.: 6029

**PETITION TO MAKE SPECIAL FOR  
NEW APPLICATION UNDER M.P.E.P.  
§ 708.02, VIII & 37 C.F.R. § 1.102(d)**

Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

Sir:

This is a petition to make special the above-identified application under MPEP § 708.02, VIII & 37 C.F.R. § 1.102(d). The application has not received any examination by an Examiner.

(a) The Commissioner is authorized to charge the petition fee of \$130 under 37 C.F.R. § 1.17(i) and any other fees associated with this paper to Deposit Account 20-1430.

(b) All the claims are believed to be directed to a single invention. If the Office determines that all the claims presented are not obviously directed to a single invention, then Applicants will make an election without traverse as a prerequisite to the grant of special status.

(c) Pre-examination searches were made of U.S. issued patents, including a classification search and a key word search. The classification search was conducted on or around October 5, 2005 covering Class 369 (subclasses 13.02, 47.14, 53.17, 53.21, and 275.3), Class 707 (subclasses 10, 100, 102, and 200-205), Class 710 (subclass 65), Class 711 (subclasses 4, 100, 111-114, and 160-162), Class 713 (subclasses 193 and 194), Class 714 (subclass 42), and Class 726 (subclass 26), by a professional search firm, Mattingly, Stanger, Malur & Brundidge, P.C. The key word search was performed on the USPTO full-text database including published U.S. patent applications. A search for foreign art was also conducted using the European Patent Office's ESPACENET database and Japanese patent database.

(d) The following references, copies of which are attached herewith, are deemed most closely related to the subject matter encompassed by the claims:

- (1) U.S. Patent No. 6,477,530 B1;
- (2) U.S. Patent No. 6,477,617 B1;
- (3) U.S. Patent No. 6,857,054 B2;
- (4) U.S. Patent Publication No. 2003/0145182 A1;
- (5) U.S. Patent Publication No. 2003/0200458 A1;
- (6) U.S. Patent Publication No. 2004/0059952 A1;
- (7) U.S. Patent Publication No. 2005/0144405 A1; and
- (8) U.S. Patent Publication No. 2005/0193034 A1.

(e) Set forth below is a detailed discussion of references which points out with particularity how the claimed subject matter is distinguishable over the references.

A. Claimed Embodiments of the Present Invention

The claimed embodiments relate to a storage system, in particular to a storage system configured to provide a reliable data archiving capability. One method for providing data verification or certification is to use Write Once and Read Many (WORM) techniques.

Independent claim 1 recites a method for operating a storage system configured to provide a Write Once and Read Many (WORM) function. The method comprises receiving a first command at a storage subsystem from a host; and storing at least a portion of the first command on a WORM storage device coupled to the storage subsystem. The WORM storage device is used to verify the WORM function of the storage system.

Independent claim 13 recites a method for providing a data archival function, comprising: storing at least portions of commands directed to a storage subsystem in a Write Once and Read Many (WORM) storage device, the commands being of a type that affects a content of data stored in a storage area of the storage subsystem; and associating a serial number to each of the commands, the serial number being useful for sorting the commands in a given order. The WORM storage device includes a plurality of command records, the command records including the at least portions of the commands and the serial numbers. The command records are useful for verifying whether or not a storage subsystem has maintain a WORM integrity.

Independent claim 32 recites a storage system coupled to a host computer. The storage system comprises a storage controller that conducts an I/O operation from the host computer; and a plurality of storage areas defined by at least one disk drive. The storage controller collects log information of the I/O operation for at least one of the plurality of storage areas when the at least one storage area is defined as a WORM area. The log information of the I/O operation is stored into a WORM storage device located separately from the WORM area.

One of the benefits that may be derived is a WORM archiving system that provides a high degree of trust, ease of management, limited performance impacts, and low implementation cost, particularly a system that enables a WORM verification or proving feature.

B. Discussion of the References

1. U.S. Patent No. 6,477,530 B1

The patent to Omata et al., US 6477530, discloses a digital data recording and reproducing system that comprises a data input part 14, a computer system unit 15, and a data

output part 37. The computer system unit 15 includes a data retention part 12 to store data and an access log recording part 4 to record that a user has accessed the data retention part on changes or corrections in the data retention part. See, e.g., column 1, line 62 to column 2, line 30; column 5, lines 41-53; and column 6, line 55 to column 7, line 17.

Omata et al. discloses a data retention part and an access log recording part. It does not relate to storing log information or commands directed to a storage subsystem in a WORM storage device. More specifically, Omata et al. fails to teach storing at least a portion of a first command received at a storage subsystem on a WORM storage device which is coupled to the storage subsystem and used to verify the WORM function of the storage system, as recited in independent claim 1; or storing at least portions of commands directed to a storage subsystem in a WORM storage device, wherein the WORM storage device includes a plurality of command records useful for verifying whether or not a storage subsystem has maintained a WORM integrity, as recited in independent claim 13; or storing log information of the I/O operation of a storage controller into a WORM storage device located separately from the WORM area of the storage system, as recited in independent claim 32.

2. U.S. Patent No. 6,477,617 B1

The patent to Golding, US 6477617, discloses a storage system for storing and retrieving data records. The system includes storage mediums 21, 31, and controllers 22, 32, and message logs 23, 33. The storage medium stores data records, the data records being indexed by addresses which specify the location of the data records in the storage medium. The storage system includes a storage device in which log information may be stored separately from the data. The log information may be stored in a non-volatile RAM or in a separate area of the disk. See, e.g., column 7, lines 39-47.

Golding discloses storing log information in a storage device separately from the data, such as a non-volatile RAM or a separate area of the disk. It does not relate to storing log information or commands directed to a storage subsystem in a WORM storage device. More specifically, Golding fails to teach storing at least a portion of a first command received at a storage subsystem on a WORM storage device which is coupled to the storage subsystem and used to verify the WORM function of the storage system, as recited in

independent claim 1; or storing at least portions of commands directed to a storage subsystem in a WORM storage device, wherein the WORM storage device includes a plurality of command records useful for verifying whether or not a storage subsystem has maintained a WORM integrity, as recited in independent claim 13; or storing log information of the I/O operation of a storage controller into a WORM storage device located separately from the WORM area of the storage system, as recited in independent claim 32.

3. U.S. Patent No. 6,857,054 B2

The patent to Minne, US 6857054, discloses a write once storage device for use with a host device. The storage device 100 comprises a write-once memory adapted to store data files; a re-writeable memory that contains a file access table; and a device controller that is configured to control the operation of the storage device such that it is responsive to the host device attempting to modify the file access table. The controller enables the file access table contained in the re-writeable memory to be modified. The storage device receives data to be stored and stores the data within the write-once memory. The file access table stored in re-writeable memory of the storage device is updated. See, e.g., column 1, lines 51-63; column 2, lines 23-40; and column 6, line 11 to column 7, line 13.

Minne discloses a storage device that includes a write-once memory for storing data. It does not relate to storing log information or commands directed to a storage subsystem in a WORM storage device. More specifically, Minne fails to teach storing at least a portion of a first command received at a storage subsystem on a WORM storage device which is coupled to the storage subsystem and used to verify the WORM function of the storage system, as recited in independent claim 1; or storing at least portions of commands directed to a storage subsystem in a WORM storage device, wherein the WORM storage device includes a plurality of command records useful for verifying whether or not a storage subsystem has maintained a WORM integrity, as recited in independent claim 13; or storing log information of the I/O operation of a storage controller into a WORM storage device located separately from the WORM area of the storage system, as recited in independent claim 32.

4. U.S. Patent Publication No. 2003/0145182 A1

The published patent application to Naito et al., US 20030145182, discloses a data storage apparatus in which tampered data or date information can be detected during later data verification, thereby verifying the correctness of the data and the date information. A portable storage medium has an erasable user area and a write-once area so that the writing unit can write the data and the time information to the user area, and the signature to the write-once area. A tamper free clock and a signature key are also provided. Thus, by setting a signature to be un-erasable, tampered data and time information can be detected with high precision. See, e.g., paragraphs [0016]-[0019], [0042], [0053], and [0055].

Naito et al. discloses writing a signature to a write-once area of a storage medium while the data and the time information are written to an erasable user area of the storage medium. It does not relate to storing log information or commands directed to a storage subsystem in a WORM storage device. More specifically, Naito et al. fails to teach storing at least a portion of a first command received at a storage subsystem on a WORM storage device which is coupled to the storage subsystem and used to verify the WORM function of the storage system, as recited in independent claim 1; or storing at least portions of commands directed to a storage subsystem in a WORM storage device, wherein the WORM storage device includes a plurality of command records useful for verifying whether or not a storage subsystem has maintained a WORM integrity, as recited in independent claim 13; or storing log information of the I/O operation of a storage controller into a WORM storage device located separately from the WORM area of the storage system, as recited in independent claim 32.

5. U.S. Patent Publication No. 2003/0200458 A1

The published patent application to Hori et al., US 20030200458, discloses a storage apparatus that can store history information associated with input and output of classified data. Each of the plurality of history information stored in the plurality of log storage units includes identification information to identify classified data. Each of the plurality of history information stored in the plurality of log storage units includes identification information to identify classified data. The administration information storage

unit stores the last record sequence number corresponding to the log entry storing history information of the latest communication. See, e.g., paragraph [0020].

Hori et al. discloses storing history information associated with I/O of classified data in log storage units. It does not relate to storing log information or commands directed to a storage subsystem in a WORM storage device. More specifically, Hori et al. fails to teach storing at least a portion of a first command received at a storage subsystem on a WORM storage device which is coupled to the storage subsystem and used to verify the WORM function of the storage system, as recited in independent claim 1; or storing at least portions of commands directed to a storage subsystem in a WORM storage device, wherein the WORM storage device includes a plurality of command records useful for verifying whether or not a storage subsystem has maintained a WORM integrity, as recited in independent claim 13; or storing log information of the I/O operation of a storage controller into a WORM storage device located separately from the WORM area of the storage system, as recited in independent claim 32.

6. U.S. Patent Publication No. 2004/0059952 A1

The published patent application to Newport et al., US 20040059952, discloses an authentication system for credit cards. The system plans to configure and enable extensive monitoring and logging services. Every authentication and transaction request along with the results are logged on a WORM media to ensure that data cannot be altered following the recording of the log entry. See, e.g., paragraph [0088].

Newport et al. is directed to a trusted authentication service provider in which authentication and transaction requests with results are logged on a WORM media. It does not relate to storing log information or commands directed to a storage subsystem in a WORM storage device. More specifically, Newport et al. fails to teach storing at least a portion of a first command received at a storage subsystem on a WORM storage device which is coupled to the storage subsystem and used to verify the WORM function of the storage system, as recited in independent claim 1; or storing at least portions of commands directed to a storage subsystem in a WORM storage device, wherein the WORM storage device includes a plurality of command records useful for verifying whether or not a storage subsystem has maintained a WORM integrity, as recited in independent claim 13; or storing

log information of the I/O operation of a storage controller into a WORM storage device located separately from the WORM area of the storage system, as recited in independent claim 32.

7. U.S. Patent Publication No. 2005/0144405 A1

The published patent application to Doran et al., US 20050144405, discloses a method to qualify access to a block storage device via augmentation of the device's controller and firmware flow. The method employs one or more block exclusion vectors (BEVs) that include attributes specifying allowed access operations for corresponding block address ranges. Logic in accordance with the BEVs is programmed into the controller for the block storage device, such as a disk drive controller for a disk drive. In response to an access request, a block address range corresponding to the storage block(s) requested to be accessed is determined. Based on BEV entries, a determination is made to whether the determined logical block address range is covered by a corresponding BEV entry. If so, the attributes of the BEV are used to determine whether the access operation is allowed. The method may be used to secure access to firmware stored on a disk drive, thus enabling a system configuration that does not require a conventional firmware storage device. The method also includes storing an audit log that can be stored into a write-only memory region of a storage device. See, e.g., paragraphs [0021]-[0024].

Doran et al. discloses storing an audit log in a write-only memory region of a storage device. It does not relate to storing log information or commands directed to a storage subsystem in a WORM storage device. More specifically, Doran et al. fails to teach storing at least a portion of a first command received at a storage subsystem on a WORM storage device which is coupled to the storage subsystem and used to verify the WORM function of the storage system, as recited in independent claim 1; or storing at least portions of commands directed to a storage subsystem in a WORM storage device, wherein the WORM storage device includes a plurality of command records useful for verifying whether or not a storage subsystem has maintained a WORM integrity, as recited in independent claim 13; or storing log information of the I/O operation of a storage controller into a WORM storage device located separately from the WORM area of the storage system, as recited in independent claim 32.



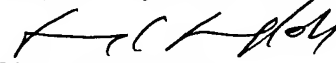
8. U.S. Patent Publication No. 2005/0193034 A1

The published application to Kitsuregawa et al., US 20050193034, discloses a disk access controller 23 to control access to magnetic disk devices under a primary storage system. An update processing portion is a processing portion in which when the received access request is a write request, it is determined whether or not the contents of the write request are log information indicating contents of the database processing executed in the database buffer of the primary host computer. If the write contents are the log information, the portion converts position information indicated in the log information into physical position information in the primary storage system. See, e.g., paragraphs [0046]-[0047].

Kitsuregawa et al. discloses converting log information into physical position information in the primary storage system. It does not relate to storing log information or commands directed to a storage subsystem in a WORM storage device. More specifically, Kitsuregawa et al. fails to teach storing at least a portion of a first command received at a storage subsystem on a WORM storage device which is coupled to the storage subsystem and used to verify the WORM function of the storage system, as recited in independent claim 1; or storing at least portions of commands directed to a storage subsystem in a WORM storage device, wherein the WORM storage device includes a plurality of command records useful for verifying whether or not a storage subsystem has maintained a WORM integrity, as recited in independent claim 13; or storing log information of the I/O operation of a storage controller into a WORM storage device located separately from the WORM area of the storage system, as recited in independent claim 32.

(f) In view of this petition, the Examiner is respectfully requested to issue a first Office Action at an early date.

Respectfully submitted,

  
Chun-Pok Leung  
Reg. No. 41,405

TOWNSEND and TOWNSEND and CREW LLP  
Two Embarcadero Center, 8<sup>th</sup> Floor  
San Francisco, California 94111-3834  
Tel: 650-326-2400; Fax: 415-576-0300  
Attachments; RL:rl

60623522 v1